BE SMARTER

Staying one step ahead of potential identity thieves crouching at your door

ABBIE DARST | PROGRAM COORDINATOR

To an identity thief, you are just another number to steal. An officer's badge and training are not deterrents in this crime. It may be easier for law enforcement officers across the commonwealth to assume their position, training and experience shelters them from being vulnerable to those lurking, ready to strip them of their identity, ruin their credit and destroy their security — but it's not smart.

Identity theft is one of the fastest growing crimes in America, catching millions of people off guard every year. Law enforcement officers are not necessarily immune, and can also find themselves picking up the pieces of their identity if they are not careful and aware of the plethora of tactics and schemes identity thieves employ.

"Offenders today are doing detective work — they do what the investigators do," said Jim McKinney, instructor at the Department of Criminal Justice Training.

Identity thieves have found the ins and outs of searching for, and obtaining, people's personal data to harvest for their own deceptive use. Though the methods of identity theft are almost innumerable, there are specific types of theft ploys of which you should be aware.

GO PHISH

Legitimate-looking emails and copycat websites from financial institutions or government agencies are the basis of phishing scams. Thieves will set up false emails and website fronts that mimic businesses and agencies that individuals would trust. They send out these emails that ask for sensitive, personal information such as social security numbers, passwords and account numbers. Oftentimes, these inquiries will even fall under the guise of keeping you safe by explaining about so-called security breeches and the need to verify information. Sometimes, the email will have a link that redirects you to a website where the information is to be entered. In a society where so much of people's correspondence is through electronic means, whether it be receiving weekly newsletters, monthly statements or frequent advertisements through email, these scams begin to look less and less fishy and throw up fewer red flags for consumers.

"Verifying information means you put in information, and they are complete scams," said Detective Burt Finley, who serves the Hopkinsville Police Department as a computer crimes investigator. "Things that can tip you off are that they ask for account numbers instead of asking to verify account numbers they provide, and there [are] just one or two places that there are slight grammar errors. Crap like that doesn't slide through on a professional site."

Simply being aware of phishing scams can help individuals make smarter choices about how they approach official-looking emails they receive. It's important to remember that legitimate companies and organizations will never ask you to verify sensitive information by email.

"If you do get these, don't enter any information," Finley said. "Never click a link. Click out and go directly to your actual site and log on directly. If there is something in there [you] need to know, it will be there for [you] in the messages section or somewhere."

Phishing scams have evolved into smishing and vishing scams, too. Smishing, like phishing, asks for confidential account information, but uses text messages sent to your phone. Vishing, or voice phishing scams are automated voice messages directing individuals to call their bank or credit card company under the pretext of clearing up a problem, like theft. A number is given to call back where they then prompt for personal account information verification.

Vishing scams can seem more legitimate because people are becoming more aware of phishing scams involving email and think that if their bank was calling them to verify information, that would be a reasonable way to obtain such verifications. One way to avoid these scams is to keep a list of the numbers to personal banks and credit companies that you can call directly, instead of calling the number provided on the received automated voice message.

BUYING THE PHARM

"Technology is making it so much easier to find this information and easier to do," Finley said. "You just have to use common sense."

Information such as maiden names, street addresses and driver's license numbers are all part of public record and a lot of companies pharm for identities, Finley said. Pharmed information is how companies tailor advertisements, mailings and other marketing tools to specific audiences. These companies use this information harmlessly, seeking only to enhance their marketability and reach those who >>